	[illegible]
	12/10/05
	[illegible]
	12/20/05
	[illegible]

Exception/SOR/ICR	

Amended on December 14, 2005

DOJ Privacy Impact Assessment (PIA)

Part One: Is a PIA required?

Instructions for Questions 1-4: If you answer "yes" to **any** of Questions 1-3 **and** Question 4, go on to the next question. If you answer "no" to **all** of Questions 1-4, please briefly describe the IT system that is at issue, and submit this document for review under the PIA process.

1. Are you developing or procuring a new IT system or project that collects, maintains, or disseminates information:

    a. about U.S. citizens or aliens lawfully admitted for permanent residence; and

    b. that does NOT pertain only to government employees or contractors?
    Yes.

2. Are you initiating a new electronic collection of information under the Paperwork Reduction Act? [1]
    No.

3. Are you making a change to an existing IT system that creates new privacy risks? For example:

    a. Are you applying a new technology to an existing system that significantly changes how information is managed in the system?
    Yes.

    b. Are you making a change in business processes:

        i. that merges, centralizes, matches or otherwise significantly manipulates existing databases?
        Yes.

        ii. that results in significant new uses or disclosures of information or incorporation into the system of additional information?
        Yes.

    c. If this information has been collected previously:

        i. Are new or significantly larger groups of people being impacted?

[1] This includes new electronic collections of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government). See 44 USC Chapter 35 and implementing regulations, 5 CFR Part 1320.8.

No. DOJ is not collecting new data about additional people. The R-DEx system will make the already collected data available more broadly to law enforcement. In so doing, R-DEx increases the ability to share information and identify and apprehend criminals.

ii. Is new data being added resulting in new privacy concerns?
No.

iii. Is data being added from a commercial or public source?
No.

4. Is this information individually identifiable? (Does this pertain to specific individuals who can be identified either directly or in conjunction with other data?) If no, submit this document for review under the PIA process. If yes, continue to the next question.

   Yes.

Instructions for Questions 5-6: If you answer "yes" to any of Questions 5-6, submit the required documentation for review under the PIA process. If you answer "no" to a question, continue on to the next question.

5. Has a PIA or similar evaluation been conducted? If yes, does the existing PIA address the questions in Part Two? If yes, submit the existing PIA with this document for review under the PIA process. If no, continue to the next question.
   No.

6. Is this a national security system as defined at 40 U.S.C. 11103? [2] If yes, please attach verification and submit this document for review under the PIA process. If no, continue to Part Two.
   No.

Part Two: Preliminary PIA (Routine database systems)

1. Please provide a general description of the system, including the purpose of the system.
   The Regional Data Exchange system (R-DEx) is a data repository that will contain criminal law enforcement information from the Department of Justice (DOJ or the "Department") components. The information contained on this system consists of sensitive but unclassified criminal law enforcement records collected and produced by the following DOJ components: the Federal Bureau of Prisons (BOP); the United States Marshals Service (USMS); and the selected field offices of the Bureau

[2] A national security system means, as defined in the Clinger-Cohen Act, an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management. See 40 U.S.C. 11103.

of Alcohol, Tobacco, Firearms, and Explosives (ATF), the Drug Enforcement Administration (DEA), and the Federal Bureau of Investigation (FBI). This information is being contributed to and maintained in this system for the purpose of sharing the DOJ's criminal law enforcement information with law enforcement personnel at all levels of government so that they can more effectively investigate, disrupt, and deter criminal activity, including terrorism, and protect the national security. This system will be accessible to all of the components contributing information and to other federal, state and local law enforcement agencies. R-DEx will have data analysis capabilities, such as (but not limited to) link analysis and geo-mapping of related incidents.

2. Please describe the types of records that will be contained in the system and the categories of individuals to whom the records pertain.
The system consists of sensitive but unclassified criminal law enforcement records collected and produced by the ATF, the BOP, the DEA, the FBI, and the USMS, including: investigative reports and witness interviews from both open and closed cases; criminal event data (e.g., characteristics of criminal activities and incidents that identify links or patterns); criminal history information (e.g., history of arrests, nature and disposition of criminal charges, sentencing, confinement, and release); and identifying information about criminal offenders (e.g., name, address, date of birth, birthplace, physical description). The system also consists of audit logs that contain information regarding queries made of the system. Aside from the audit logs, all information in R-DEx represents copies of files from source component systems.

Individuals covered by this system include individuals who are or were referred to in potential or actual cases or matters of law enforcement concern to the ATF, the BOP, the DEA, the FBI and the USMS. Because the system contains audit logs regarding inquiries, individuals who use the system to conduct such queries are also covered.

3. What is the volume of records that will be contained in the system, including approximate number of people impacted?

Estimated Total Number of Records: 1 million+

Possible # of persons impacted: Anywhere from 750,000 to 1 million at this time. Many of the records might duplicate information or consist of multiple entries about individuals. The number of records is expected to increase based on the periodic data uploads and could potentially increase the number of individuals impacted.

4. What is the purpose for which the system data will be used, including how it will be used and who will use it?
This system is maintained for the purpose of ensuring that users have access to information from regional law enforcement agencies of all levels in a systematic and ongoing manner to maximize the benefits of information gathering and analysis

needed to respond to criminal threats, to support law enforcement activities, to enhance public safety and to enforce protection of the nation's critical infrastructure.

FBI will administer the repository. Each participating DOJ component will contribute information to R-DEx. Additional contributing law enforcement agencies to the R-DEx system may be added at a later time. Federal, state and local law enforcement entities will use R-DEx to make queries of structured and unstructured, free-text data regarding individuals under investigation for criminal activity. R-DEx will also have data analysis capabilities, such as link analysis and geo-mapping.

5. What are the sources of the information?
Records in R-DEx are copies of the criminal law enforcement files and records systems of the participating DOJ components (i.e. ATF, BOP, DEA, FBI, and USMS). The sources for the DOJ components' information may include protected sources, witnesses, contacts, other human and technological assets, walk/call/write-ins or any other lawful method used to collect law enforcement information.

6. With whom will the information be shared outside of the Department?
The information will be shared with other federal, state and local law enforcement entities in selected geographic areas of the country so that those entities can more effectively investigate, disrupt, and deter criminal activity, including terrorism, and protect the national security.

As such, information from R-DEx may be disclosed:

(1) To any criminal, civil, or regulatory law enforcement authority (whether federal, state, local, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

(2) To a governmental entity lawfully engaged in collecting criminal law enforcement, criminal law enforcement intelligence, or national security intelligence information for law enforcement or intelligence purposes.

(3) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system of records.

(4) In an appropriate proceeding before a court, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(5) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings.

(6) To the news media and the public pursuant to 28 C.F.R. § 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(7) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

(8) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(9) To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

(10) To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

(11) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

(12) To any person or entity if deemed by the Department to be necessary in order to elicit information or cooperation from the recipient for use by the Department in the performance of an authorized law enforcement activity.

(13) To any individual, organization, or governmental entity when it is necessary to notify them of a serious terrorist threat for the purpose of guarding against or responding to such a threat.

7. Is providing information voluntary by the individuals? If yes, are individuals informed that they may decline to provide information?
No. The information pertaining to individuals is based on their suspected involvement with criminal case investigations and law enforcement concerns.

8. Do individuals have an opportunity to consent to particular uses of the information? If yes, how can individuals grant consent?
   No. There is no general opportunity to consent to particular uses of information because the information contained in the system is existing data that was lawfully gathered and maintained based on law enforcement authority and individuals may not have an opportunity to consent to particular uses of that information.

9. How will the information be secured (e.g., administrative and technological controls)?

   Information in this system is safeguarded in accordance with applicable laws, rules, and policies, including the Department's automated systems security and access policies. Records and technical equipment are maintained in buildings with restricted access. Passwords, password protection identification features, and other system protection methods also restrict access to information in this system. Only DOJ personnel and other users who are members of law enforcement agencies, have undergone background and criminal history checks, and have received appropriate training will be permitted access to the system; and such access is limited to those who have an official need for access in order to perform their duties.

   The implementations of several administrative and technological controls secure the information contained within R-DEx. The Security Administrator and the System Administrator are two major components of the R-DEx administration. The Security Administrators are responsible for viewing, monitoring, and archiving security logs and audit trails and may also be given the ability to add, change, or delete users and their system access privileges. The System Administrators are responsible for the maintenance and operation of the system as a whole, including backing up the system and its recovery.

   The R-DEx repository is physically protected in compliance with Department of Justice guidelines for Information Technology Security (DOJ 2640.2E) pertaining to both physical and environmental security. Hardware and electronic media used in the R-DEx system is protected in accordance with the sensitivity of the data, which the system is authorized to process, store, or transmit. All R-DEx hardware components and electronic media have external classification markings.

   R-DEx is also protected by boundary protection devices (e.g., firewalls and trusted guards) at identified points of interface with networks or systems (e.g. LInX). The R-DEx system employs virus protection software, encryption technology during transmission to ensure data security, and intrusion detection systems. Intrusion detection systems operate in a manner that is compliant with Title 18, Section 2511 of the United States Code, and the Electronic Communications Privacy Act.

   All access tools will enforce tight controls over which privileges a user is granted and under what conditions these privileges can be used. Wherever possible, user roles and access restrictions will be standardized across agencies.

The determination of appropriate users and assignment of passwords are other administrative controls in place. Users will also receive training on privacy and proper use of the R-DEx system.

Finally, the Memorandum of Understating (MOU) regarding the "One DOJ Information-Sharing Pilot Program" that governs use of R-DEx information stipulates how recipients can use data shared via R-DEx. One stipulation states that no law enforcement action can be undertaken until coordinated with the originator of information in R-DEx.

10. Is this information covered by a Privacy Act System of Records Notice? [3] If yes, provide the Federal Register Citation. If not, is one being created?
Yes. Federal Register, Volume 70, No. 131, July 11, 2005, and the modification may be found at Federal Register at 70 FR 72315 (December 2, 2005.

11. Is this information covered by a Computer Matching Agreement? [4] If yes, please attach.
No.

12. Is this a Major Information System as defined in OMB Circular A-130 and A-11 (Section 300-4).[5] If yes, please include identifying information and complete Part Three.
Yes. As defined a "Major information system" embraces "large" and "sensitive" information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, or its (v) significant role in the administration of an agency's programs, finances, property or other resources.

R-DEx requires special management and attention because of its importance to the agency mission since R-DEx supports the law enforcement information sharing strategy and mission of the DOJ.

13. Is this system of such significance or sensitivity (i.e., medical records, taxpayer information, etc.), or is the impact on privacy such that the system requires special consideration of privacy risks? If yes, please briefly explain and complete Part Three.
Yes. R-DEx will contain information lawfully collected and maintained as a result of criminal law enforcement investigations. These records may include sensitive

[3] The Privacy Act of 1974 requires agencies to inform the public of the existence of systems of records containing personal information. See 5 U.S.C. 552a.
[4] Under the Computer Matching and Privacy Protection Act of 1988, agencies are required to conclude written agreements specifying the terms under which matches are to be done. See 5 U.S.C. §§ 552a(8-10), (e)(12), (o), (p), (q), (r), (u).
[5] Major Information Systems include "large" and "sensitive" information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency's programs, finances, property or other resources.

personal information regarding a person's possible involvement in criminal activity, and to a limited extent a person's medical records and/or financial records depending on the nature and scope of the investigation.

14. Analysis: PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.
R-DEx information will be used for official criminal law enforcement and national security purposes only. R-DEx information cannot be accessed or used for any other purpose, including general licensing, employment, eligibility for federal or state benefits, and background investigations. R-DEx information may not be disclosed in response to a request made under any state or local access law. Information in R-DEx is discloseable only in accordance with federal law, including the Freedom of Information Act and the Privacy Act.

User limitations were created to ensure that R-DEx is used for law enforcement purposes only and only law enforcement individuals with a "need to know" the information contained within the system will have access to the R-DEx system. All applicants for the R-DEx system must undergo a background check. In addition, the above-mentioned security controls, both administrative and technological, controls were developed and implemented in order to reduce the risk of unauthorized access to the data.

Part Three: Further Analysis (Major Information Systems, etc.)

1. Please briefly describe the impact on privacy.
The R-DEx system will contain a range of information about U.S. citizens, non-U.S. citizens and other persons in this country who are referred to in potential or actual cases or matters of concern to the contributing DOJ components. Examples of information in the system include: suspected criminal activity, financial records, medical records, juvenile records, and other personal information (i.e. address, phone, social security number, etc.). All of this information will be shared internally within DOJ and externally with other federal, state and local law enforcement authorities. This information has already been lawfully collected as part of DOJ law enforcement activities. The R-DEx system only will assist in disseminating the information to other law enforcement agencies for the purpose of improving the enforcement of U.S. laws.

If an investigator or analyst determines that the information in R-DEx may be relevant to an investigation, he/she may request permission from the contributing agency to utilize the information.

Due to the volume of records and the type of information being shared, privacy rights of individuals could be impacted if the system is misused or unauthorized persons gain access. The impact on the privacy of individuals, however, will be the same as the impact of any current case analysis and investigation that includes the same data obtained from the source law enforcement agencies.

2. Please describe the alternatives to design, collection, and handling of the information that would have a lesser impact on privacy and the rationale for not selecting each such alternative, as well as the final decision.
There are two possible alternatives to handling of this information that would have lesser impact on the privacy of individuals. The first would be to not create a system like R-DEx. Based on the needs of the law enforcement community to share investigative information in order to protect citizens from criminal and terrorist activity, this is not a practical alternative.

The second would be to create a "Pointer Only" system. This means that when a query was conducted, the database would retrieve information that would list the name of the investigator or Point of Contact for the information for the user to contact. A "Pointer Only" system does not meet the needs of law enforcement entities because it may be overly burdensome and time consuming to contact the investigator or point of contact for the information that an user would seek. The retrieval of comprehensive case reports from R-DEx is more useful to law enforcement agents because they can look at the information and see if it is related to their case and not have to call a point of contact unless they think it is relevant. Because speed is often an important element in apprehending a criminal or preventing a criminal act, "pointer systems" may limit law enforcement's ability to effectively combat crime. They also do not allow for the use of analytical tools. In order to expedite the information sharing process across varying federal, state, local, tribal law enforcement entities and effectively investigate criminal activity, it is necessary to create a system such as R-DEx without a "Pointer Only" design.

3. What measures are in place to mitigate identified risks?
Information in this system is safeguarded in accordance with applicable laws, rules, and policies, including the Department's automated systems security and access policies. Records and technical equipment are maintained in buildings with restricted access. Passwords, password protection identification features, and other system protection methods also restrict access to information in this system. Only DOJ personnel and other users who are members of law enforcement agencies, have undergone background and criminal history checks, and have received appropriate training will be permitted access to the system; and such access is limited to those who have an official need for access in order to perform their duties.

The DOJ has implemented administrative and technological security controls and measures to protect the information collected by the government, both while in storage and in transit. These measures are designed to thwart unauthorized access and inappropriate disclosure. Other administrative and technological controls are described in more detail in Part Two, Question 9.

The R-DEx system includes robust audit capabilities. R-DEx users will periodically review the audit logs to ensure appropriate access to and use of information.

The MOU for the "One DOJ Information-Sharing Pilot Program" and joint MOUs with other agencies outline policies and procedures for the handling of information. The policies and procedures cover the actions of contributing agencies (e.g., data accuracy), as well as how recipients can use data shared. R-DEx users will also receive training on privacy and proper use of the R-DEx system.

The MOUs that enable the use of R-DEx also include sanctions for misuse of the system and/or data. Sanctions can be applied to an individual or entire agency, depending on the circumstances and severity of the misuse.

4. How will data be collected from sources other than Department records and individuals and be verified for accuracy?
   Data is currently limited to that contributed from existing DOJ records.

   The DOJ contributing agencies have the duty, sole responsibility, and accountability to make reasonable efforts to ensure that information in R-DEx is accurate, complete, timely, and relevant.

   Each individual contributing agency is responsible for ensuring and verifying accuracy with the information it is providing to the Department. Investigators verify the information within that particular contributing agency. Then the contributing agency will conduct periodic file reviews in order to verify the information.

5. How will data be checked for completeness?
   The information will be checked for completeness by the contributing agency during its periodic file reviews. Data will be as complete as allowed by the limits of the agencies' investigators.

6. Is the data current? How do you know?
   Yes. Each contributing agency is responsible for ensuring that all of the incoming documents for R-DEx are current. System user guidance establishes that the information either be dated within five years of the date at the time of uploads or current with the life of the data (i.e. new materials for an ongoing case of 10 years), whichever is longer. Each contributing agency is also responsible for updating their investigative records as new information becomes available. As such happens, the information in R-DEx will also be updated.

7. Are the data elements described in detail and documented? If yes, what is the name of the document? If not, please do so.
   Information that will be disclosed outside of the Department via R-DEx consists of unstructured free-text files and in some instances structured files. The data elements are described in detail and documented in the "R-DEx System Design" and "R-DEx Data Conversion Plan" documents.

8. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
   Information in this system is safeguarded in accordance with applicable laws, rules, and policies, including the Department's automated systems security and access policies. Records and technical equipment are maintained in buildings with restricted access. Passwords, password protection identification features, and other system protection methods also restrict access to information in this system. Other administrative and technological controls are described in more detail in Part Two, Question 9.

   Only those DOJ personnel and other users who are members of law enforcement agencies, who have undergone background checks and who have received appropriate training, will be permitted access to the system; and such access is limited to those who have an official need for access in order to perform their professional duties.

   All individuals working on the design, development, or deployment of the R-DEx system will have personnel security clearances commensurate with the level of information stored in the repository.

   Any contributing agency user that is determined by the "One DOJ" Governance Board to be in systemic or repeated violation of applicable laws and procedures governing access to and use of R-DEx information may be denied access to the R-DEx system by the "One DOJ" Governance Board.

9. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Please explain.
   Not applicable.

10. How will the data be retrieved? Can it be retrieved by a personal identifier? If yes, explain.
    Data will be retrieved from R-DEx based on a user making a query of particular information and the system identifying what documents contain the requested information. The system user can then request to view the specific documents. Records can be retrieved by the name and/or other identifier(s) of the individual.

11. What are the potential effects on the due process rights of individuals of: consolidation and linkage of files and systems; derivation of data; accelerated information processing and decision making; use of new technologies?
    The development and use of R-DEx does not adversely impact the due process rights of individuals. Law enforcement agencies have always been able to share information with other law enforcement agencies as appropriate. R-DEx facilitates this sharing and makes it more efficient by consolidating the information into one data repository and in some instances structuring the information. The use of data conducted by investigators does not change. Investigators and law enforcement authorities will use the information to investigate and potentially prosecute any

criminal suspects. If an investigator or analyst determines that the information developed as a result of a query is relevant to an investigation, the information can be used to assist with an investigation. As individuals have no right to prevent the appropriate sharing of information between law enforcement agencies, the use of R-DEx does not impact the due process rights of individuals.

To be sure, the data in the system will be made available to a larger group of law enforcement officers than previously. Officers who formerly had minimal access to sensitive law enforcement information originating from other law enforcement agencies may now have access to the information quickly and easily. There could be an increased risk of inadvertent misuse of information. The impact on the privacy of individuals, however, will be the same as the impact of any current case analysis and investigation that includes the same data obtained manually from other law enforcement agencies. Any possible effect on an individuals' due process rights would occur as a result of a criminal prosecution and procedures, not as a result of the ability to query the data in R-DEx.

12. How are negative effects to be mitigated?
    This is not applicable. The Department has determined that there is no adverse impact on the due process rights of individuals caused by the operation and use of the R-DEx system.

13. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?
    The Department will restrict access to the R-DEx system to authorized law enforcement personnel with a need for access such as supervisors, law enforcement agents/officers, and task force members associated with agencies that have signed the MOU. In addition, limited access to the R-DEx system will be provided to system administration and system security personnel for purposes of conducting system operation and maintenance tasks. All such personnel (either government employees or contractors/subcontractors) shall be vetted and cleared for system access and their access shall be monitored and audited.

14. How will the determination be made as to who will have access to the data?
    The Deputy Attorney General, in consultation with the Department components participating in the R-DEx system, will determine who can have access to information in the R-DEx system. The Department will document these determinations in the MOU. In accord with the MOU, chiefs of partner agencies will authorize specific persons to access information in R-DEx consistent with the determinations made by the Deputy Attorney General.

    Access to R-DEx data by system administrators and/or system security officers will be limited to only that needed to perform these functions and will be documented in the MOU regarding the R-DEx system.

15. Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes. Criteria, procedures, controls and responsibilities are documented in the MOU and in R-DEx system administration and security documentation.

16. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?
R-DEx has an audit capability that will log the date, time, subject, and originating account of all user queries. The parties will maintain these audit logs for five years or for the life of the records accessed, whichever is longer. The R-DEx security staff will also review these audit logs.

Training will be required for all R-DEx users (including those accessing R-DEx information from other systems). The training will include procedures to ensure users know how to properly use R-DEx information. This training will be provided to make users of R-DEx information aware of what information can be accessed from R-DEx and will include a description of the information contained in the system, a typology of DOJ investigative reports, third-party rules, and coordination requirements, and other appropriate information. Users will also be notified of potential sanctions for misuse of the system or any data obtained from the system.

17. Do other systems share data or have access to data in this system? If yes, explain.
Yes. DOJ intends to connect R-DEx to other regional law enforcement information sharing systems

18. Who will be responsible for protecting the privacy interests of individuals affected by the interface?
All users and the participating agencies of R-DEx will be responsible for protecting the privacy interest of individuals identified in the system. These responsibilities are identified in the MOUs and will be reiterated to each user through training.

Each DOJ component that contributes records to R-DEx will periodically audit access by other agencies to ensure appropriate use of the information. Each participating DOJ component will review its own use of the R-DEx system and will take action to address any misuse.

Each contributing agency is responsible for the actions of its users, and sanctions will be applied for intentional or repeated misuse of the system and/or the data contained within. The "One DOJ" Governance Board will determine appropriate sanctions.

19. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?
Yes. Generally, the agencies that have entered the MOU with DOJ will share or have access to R-DEx.

20. Who is responsible for assuring proper use of the data?

The contributing agency has the sole responsibility to ensure that information in R-DEx was not contributed or maintained in violation of any applicable law by the contributing agency.

All users and the participating agencies of R-DEx will be responsible for ensuring appropriate use of information made available through the system. These responsibilities are identified in the MOUs and will be reiterated to each user through training. Each partner agency is responsible for the actions of its users, and sanctions will be applied for intentional or repeated misuse of the system and/or the data contained within. Each DOJ component that contributes records to R-DEx will periodically audit access by other agencies to ensure appropriate use of the information. Finally, each participating DOJ component will review its own use of the R-DEx system and will take action to address any misuse.

The contributing agency has the sole responsibility to ensure that information in R-DEx was not contributed or maintained in violation of any applicable federal, state, or local law by the contributing agency.

21. What are the retention periods of data in this system?
Records in this system in all formats are maintained and disposed of in accordance with appropriate authority of the National Archives and Records Administration.

Each contributing agency is responsible for its data. R-DEx system administrators will only update and/or delete data per the update process. The agencies control what is updated, added, modified or deleted. No information is removed unless it is deleted through the update process by the contributing agency.

System user guidance outlines that the retention period be at least five years from the date of the upload or the life of the record whichever is longer.

22. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?
Records in this system in all formats are maintained and disposed of in accordance with appropriate authority of the National Archives and Records Administration.

Each contributing agency is responsible for its data. The system administrators will eliminate data only per the update process. The agencies control what is deleted. No information is removed unless it is deleted through the update process by the contributing agency.

23. Is the system using technologies in ways that the Department has not previously employed? If yes, how does the use of this technology affect individual privacy?
Yes.

DOJ components will be sharing their sensitive but unclassified criminal law enforcement information with other federal, state and local law enforcement

agencies. R-DEx provides a single interface through which DOJ components will exchange information with authorized law enforcement agencies. The system also will assist agents and officers to compare records and analyze the contents of those records to determine similarities or other relationships between criminal acts and the people suspected of committing these acts. R-DEx will provide analytical tools that can be used to correlate case information across records, for example geographic mapping and link analysis.

If abused or misused, the R-DEx system could have a negative impact on an individuals' privacy. The contributing agencies have agreed to policies and procedures to mitigate any risks.

R-DEx information, including analytical products derived there from, may not be used as a basis for action or disseminated for any other purpose or in any other manner outside the contributing agency that accessed the information, unless that agency first obtains the permission of the contributing agency. Specifically included within this prohibition is any inclusion of R-DEx information in an official investigative or case file, and any use of R-DEx information in the preparation of judicial process such as affidavits, warrants, or subpoenas.

Immediate dissemination of R-DEx information can be made without written permission if the agency that accessed the information determines that:

(a) there is an actual or potential threat of terrorism, immediate danger of death or serious physical injury to any person, or imminent harm to the national security; and

(b) it is necessary to disseminate such information without delay to any appropriate recipient for the purpose of preventing or responding to such a threat.

24. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain and indicate what controls will be used to prevent unauthorized monitoring.
No. The R-DEx system will provide the capability to identify individuals, addresses and vehicles whose attributes meet the results of a query and provide information on the individuals, addresses and vehicles if that information is contained in the data responsive to the query. However, the system has no mechanism for monitoring the real-time actions, the identification or the location of individuals.

25. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain and indicate what controls will be used to prevent unauthorized monitoring.
No. See response for Part Three, Question 24 above.